Malcolm Baldrige National Quality Award
2009 Award Recipient
Honeywell FM&T

Protecting Export Controlled Information

NNSA

Honeywell

The Department of Energy's National Security Campus is operated and managed by Honeywell Federal Manufacturing & Technologies, LLC under contract number DE-NA0000622

Introduction

- Effective July 1, 2014 Honeywell FM&T articles and technical data previously covered under the International Traffic in Arms Regulations (ITAR) changed agency jurisdiction.
  - From Department of State (DOS) to Department of Energy (DOE)
  - Still considered military defense article
  - No U.S. government registration requirements under DOE
  - Same restrictions: No Foreign Person Access

Agency Jurisdiction

Department of Energy (DOE)	Department of State (DOS)	Department of Commerce (DOC)
Atomic Energy Act (AEA)	Int'l Traffic In Arms Regulations (ITAR)	Export Administration Regulations (EAR)
Nuclear Weapon or NW related items	Military defense articles, service and technology	Dual-Use articles and technology
*Tier *Guidance*	U.S. Munitions List (USML)	Commerce Control List (CCL)

Effective July 1, 2014 →

What is an Export?

An **export** is the transfer of hardware, technical data or technical assistance to anyone who is not a citizen or *legal resident* of the United States, regardless of the location in which the transfer occurs.

"Transfer"	Includes physical, electronic, and oral transmission, or visual inspection. (Technology support via telephone, fax, or email)
"Hardware"	Includes end items, manufacturing equipment, test equipment, tooling, raw materials.
"Technical Data"	Includes drawings and manufacturing processes, specifications, installation instructions, user manuals, other documentation, and software.
"Technical Assistance"	Includes any training or guidance on products, processes, and data (also known as defense service).

The transfer of such items/information to foreign persons, where ever located, is considered an export.

Deemed Export Controls

Other Types of an Export

Deemed Export :

- When disclosing export controlled information of an item or technical data to a foreign person, wherever located, it is “deemed” to be an export to their home country.

Deemed Export Exceptions:

Any foreign national is subject to the "deemed export" rule **except** a foreign national who is granted:

1. Permanent residence, as demonstrated by the issuance of a permanent resident visa (i.e., "Green Card")
2. U.S. citizenship
3. Status as a "protected person"

Technology Matrix

Types / Forms	Development Technology	Production Technology	Use Technology
Tangible Technology	Original blue print for controlled item	Written manufacturing instructions to produce controlled item	Written instructions to run controlled item
Intangible Technology	Discussion about the layout of a controlled item	E-mail regarding the testing of controlled item	Verbal instructions on the repair of controlled item

Controlling Information – Technology Control Plan

We identify "what" expectations,

Your written procedures must describe "how" these expectations are met.

Who is impacted by the receipt of ECI?

- Manufacturing
- Purchasing
- Shipping and Receiving
- IT
- Quality inspection
- Human Resources
- Foreign owned parent companies
- Receptionist

Risk Assessment

- Take a tour of your own facility: look for access points
- Discuss with employees who provide tours to non-employees
- Do contractors, vendors, truckers have open access to your facility
- Are employee's familiar with what is meant by export controlled information
- Who identifies if your company is receiving ECI
  - How is it controlled once received
- Are employees aware when foreign visitors are at your facility
  - How are they identified
  - Are visitors allowed access to your company computer
- Do you ask or does your visitor log identify citizenship

Risk Assessment

- Are drawings located on the shop floor
- What restrictions are flowed down to sub-tier suppliers
- Does your company host training for customers onsite
- Does your company have a clean desk policy
- Where is your server located
  - Where are documents stored once received
  - Does your foreign parent company have access to tech data
- How is export controlled technical data electronically released
- Who do employees contact regarding questions related to foreign persons or potential red flags

Access Controls

Supplier shall establish written operating procedures and physical security measures designed to protect inadvertent release or disclosure to foreign persons or other unauthorized third parties.

- **ACCESS** No access is allowed by foreign persons to FM&T products, technical data, or products built from FM&T technical data including supplier's foreign person employees, consultants, visitors and/or subcontractors.

- Supplier shall *only* allow U.S. persons to have access to FM&T products or technical data, and only U.S. persons will be allowed to perform any work on behalf of FM&T, unless permission is obtained otherwise from FM&T Export Control Office.

- Suppliers shall ensure that the individual with whom the discussion of information provided by FM&T is to be held, or to whom the information is to be transferred, is not a foreign person.

Exception: foreign persons who are permanent resident (green card holders) are not prohibited access.

Access Controls

- Supplier shall take steps to ensure that other **persons working on behalf of** supplier in connection with performance against our purchase orders do not engage in any actions that might result in the diversion of any products.

- Supplier shall maintain documents evidencing current **employees' eligibility** status to work in the United States and provide these documents to FM&T upon FM&T's request.

- **Servers** shall be hosted in the United States and maintained by U.S. persons. Supplier shall maintain adequate controls in its information technology system to protect against unauthorized access, disclosure and transfer of FM&T technical data and software.

Things to Consider

- Access by visitors, cleaning company, vendors, contractors, new hires
  - Do you identify if they are foreign persons
- What access is given to visitors of company computer
- Tours – how do your restrict access from casual viewing
  - How do you restrict foreign person access from ECI documents while in use during production
  - Foreign parent company access restricted

Best Practices – Security Access

Depends on the size of your company

- Visitor log is not enough – identify when visitor arrives
  - Does your sign-in sheet ask for country of citizenship; foreign residency
- Restrict cell phone use, photographs while on tours
- Escort visitors; limit access for delivery drivers to an area
- Manufacturing doors opened during business hours – monitor doors
- Tour planned – at a distance
- Restricted area for production of export controlled items
- Clean desk policy for employees
- Policy for no technical data thrown in the trash

Storage Controls

- STORAGE of FM&T information shall be maintained within a secure area. Such areas include a locked receptacle such as a file cabinet, desk drawer, overhead furniture credenza system, or similar locked compartment.

- FM&T information can also be stored in a room or area that has sufficient physical access control measures (guard, cipher lock, card reader, etc.) to afford adequate protection and prevent unauthorized access from foreign persons.

- *Companies who host their servers or store email on the "cloud" will not be approved to receive export controlled information from FM&T*

Best Practices - Storage

Electronic or Paper

- Electronic storage where ECI is stored – limit who has access to the files to those who have a need to know
- Document control room – check in/out policy
- Locked storage cabinet or storage area
- Who has access to the locked area
- Cover up technical data together with parts or limit the information contained on travelers

Secure Handling

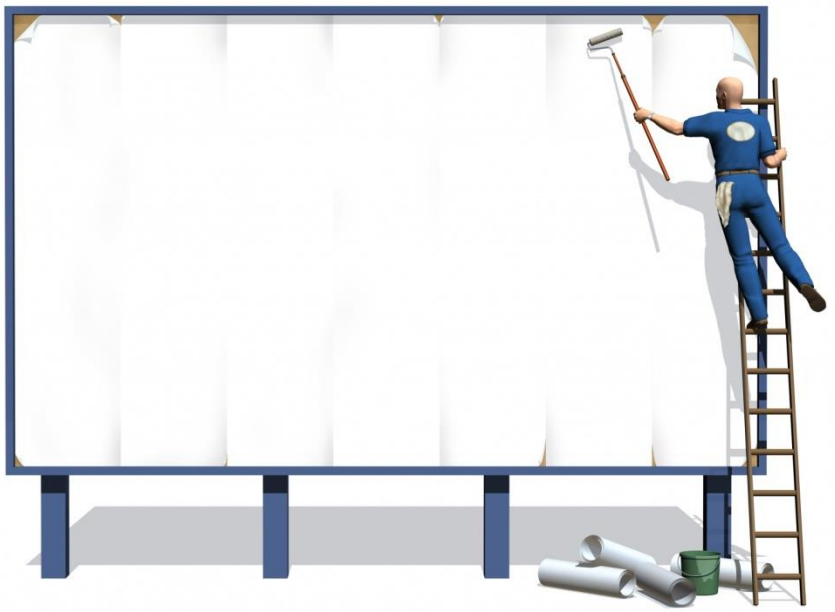
- TRANSMISSION of FM&T technical data will be sent electronically through a secured method of transmission. (e.g. Email encryption or authorized users of Web Exchange) Supplier is responsible to send FM&T technical data through secure methods when transmitting electronically.

- DESTRUCTION of FM&T information including gerber files and electronic storage media, when no longer needed, may be accomplished by shredding into strips, burning, pulping, or pulverizing beyond recognition or reconstruction. After destruction, material may be disposed of with normal waste.

- Articles returned for credit, failed inspection or defective parts will require demilitarization (DEMIL) in accordance 10 CFR part 109 rending useless the product. Supplier who do not have the ability to DEMIL on site should contact FM&T to obtain an export control approved recycling company.

Publicity

- FM&T products cannot be used for advertising
  - Posters
  - Product Display
  - Website
- FM&T products should not be discussed with visitors on visitor tours



Publicity

Although we understand your business need to advertise your technical capabilities, suppliers may not use items or information produced for or provided by FM&T for this purpose. This includes advertising posters, display cases and supplier websites.

FM&T products and information should not be on display during a visitor tour.

Suppliers are not allowed to reference FM&T or the Kansas City National Security Campus, on their web-based or printed materials.

Training

No access control program can succeed without proper training. Can't train entire corporation to be experts but you can train on Red Flags!

Training methods should, at a minimum, include:

- Orientation for new employees;
- Receptionist
- Shipping / Receiving
- IT
- Human Resources
- Purchasing
- Sales
- Manufacturing

Internal Notification

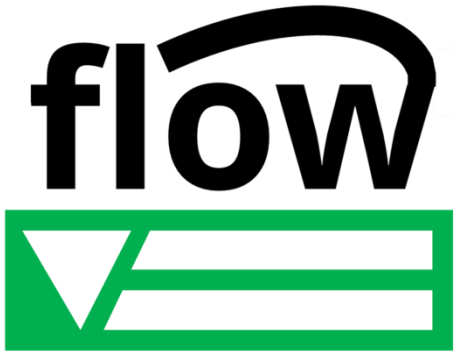
When company personnel suspect that questionable, unauthorized or illegal activities may have taken place, or that the customer is asking them to participate in such activities, a designated person within your company should contact the U.S. regulatory authority.

Audits

SITE INSPECTION

- FM&T shall conduct on-site security inspections of the supplier's facilities and ensure documented access control operating policies restricting foreign person access are in place.
  - FM&T and supplier agree to establish dates for those activities that are mutually satisfactory to each party.

- Supplier is responsible to flow down foreign person restricted access control requirements to their subcontractors. It is the responsibility of the supplier to select a subcontractor who can securely protect and handle export controlled technical data that may be shared.



In the interest of National Security we are relying on your company to handle export controlled information provided in accordance with U.S. export control laws.

Contact
Export Compliance
export@kcnsc.doe.gov